UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/240,934	01/29/1999	YAIR BARTAL	2-5-7	7975

7590 02/27/2002

RYAN & MASON
90 FOREST AVE
LOCUST VALLEY, NY 11560

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/27/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)
09/240,934	Bartal et al
Examiner	**Art Unit**
Christopher Revak	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____

2a) ☐ This action is **FINAL.** 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) 1-38 is/are pending in the applica

4a) Of the above, claim(s) 9-28, 36, and 37 is/are withdrawn from considera

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) 1-8, 29-35, and 38 is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☒ Claims 9-28, 36, and 37 are subject to restriction and/or election requirem

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

NORMAN M WRIGHT
PRIMARY EXAMINER
AU 2131

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)
16) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s). 4
18) ☐ Interview Summary (PTO-413) Paper No(s). _____
19) ☐ Notice of Informal Patent Application (PTO-152)
20) ☐ Other:

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement submitted is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Election/Restriction

2. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-8,29-35, and 38 are drawn to generating a security policy/rules that determine/define the ability of a host to send and receive packets, classified in class 713, subclass 202. The disclosed subject matter falls under the subclassification because the criteria states "means or steps for providing system security at network level."

II. Claims 9-17 and 18-28 are drawn to utilizing a model topology/definition language to produce an entity relationship model, classified in class 717, subclass 104. The disclosed subject matter falls under the subclassification because the criteria states "means or steps for designing and specifying a representation of the structure and desired behavior of a program to be developed."

III. Claims 36 and 37 are drawn to parsing to create an entity relationship model, classified in class 717, subclass 143. The subject matter falls under the subclassification because the criteria states "means or steps for analyzing program code text to determine whether the program code conforms to grammatic rules of the programming language."

3. Inventions are distinct from each other and are related because of the following reasons: Inventions I, II, and III are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I is drawn towards generating a security policy/rules that determine/define the ability of a host to send and receive packets wherein invention II recites of utilizing a model topology/definition language to produce an entity relationship model and invention III recites of parsing to create an entity relationship model. See MPEP § 806.05(d).

4. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Groups II and III, restriction for examination purposes as indicated is proper.

5. During a telephone conversation with Kevin Mason on February 22, 2002 a provisional election was made without traverse to prosecute the invention of Group I, claims 1-8,29-35, and 38. Affirmation of this election must be made by applicant in replying to this Office action.

Claims 9-17, 18-28, 36, and 37 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371© of this title before the invention thereof by the applicant for patent.

7. Claim 29 is rejected under 35 U.S.C. 102(e) as being anticipated by Reid et al.

Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of roles)(col. 2, lines 8-17). Various commands (definitions) are shown by Reid et al for setting up access control rules that are applied to the regions (assignment of roles) in column 11, denoted in the upper part of the page.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-8, 19-28,30-35, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reid et al in view of Grennan.

As per claim 1, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of roles)(col. 2, lines 8-17). Various commands (definitions) are shown by Reid et al for setting up access control rules that are applied to the regions (assignment of roles) in column 11, denoted in the upper part of the page. The teachings of Reid et al fail to disclose of generation of a configuration file for a firewall. It is disclosed by Grennan of setting up (generating) a configuration file for a firewall (section 4.2). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a configuration file for a firewall since it is known in the art that a configuration file for a firewall dictate the how the firewall functionality is to be performed. Although Reid et al is silent on the use of a

configuration file, it is essential that a configuration file exists in the teachings since it is notoriously well known that configuration files for a firewall are used to performed the intended functionality, namely setting up a security policy that is to be enforced whereby the teachings of Grennan are relied upon for showing the use of a configuration file for a firewall since it is not explicitly disclosed by Reid et al.

As per claims 2 and 31, Reid et al shows a plurality of firewalls in Figures 1a and 1b which are in defined regions (assignment of roles)(col. 1, lines 54-56). Grennan is relied upon for disclosing the use of a configuration file (section 4.2).

As per claim 3, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of roles)(col. 2, lines 8-17). The network capabilities are dictated for the services of the regions (col. 20, lines 39-44).

As per claims 4, 5, 32, and 33, Reid et al discloses of an interface card (belonging to respective hosts), VPNs, groups of VPNs, or any groupings thereof to exist in the regions (assignment of roles)(col. 5, lines 3-13).

As per claims 6 and 34, it is disclosed by Reid et al of providing policies for a plurality of regions to restrict communications to and from each of the regions. The teachings of Reid et al

are silent on providing a visual representation of the structure of the hosts in the network. The examiner hereby asserts that it would have been obvious to in means for including a visual representation of the of the structure of the hosts in the network. It is suggestive of providing a visual representation of the structure of the hosts in the network where it is taught by Reid et al that a visual means is provided by which access control (rules of the configuration file) can be defined (col. 7, lines 8-12 and 24-27) and also disclosed of GUI is used as a means to dictate how the rules are implemented (col. 8, lines 33-36) wherein the representation of the hosts in the network can be examined since there exists groupings of networks and VPNs in different regions wherein a specific security policy is applied thereto (col. 4, line 66 through col. 5, line 5). By providing a visual representation of the topology of the hosts in the network, the hosts belonging to a particular region can be easily identified and have certain access control rules applied as suggested by Reid et al.

As per claim 7, it is disclosed by Reid et al that a visual means (representation) is provided by which access control (rules of the configuration file) can be defined (col. 7, lines 8-12 and 24-27).

As per claims 8 and 35, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of

roles)(col. 2, lines 8-17). Various commands (definitions) are shown by Reid et al for setting up access control rules that are applied to the regions (assignment of roles) in column 11, denoted in the upper part of the page. The teachings of Reid et al fail to disclose of a compiler for generation of a configuration file for a firewall. It is disclosed by Grennan of setting up (generating) a configuration file for a firewall and compiling (by means of a compiler) the kernel (section 4.2, 5.1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a compiler for generating a configuration file for a firewall since it is known in the art that a configuration file for a firewall dictate the how the firewall functionality is to be performed. Although Reid et al is silent on the use of a compiler for generation of a configuration file, the teachings of Reid et al are suggestive of compiling wherein it is disclosed of ACLs (rules) used by the kernel for building, modifying, deleting, and querying the rules (col. 8, lines 20-23) which would need compiled. It is essential that a compiler for generating a configuration file exists in the teachings since it is notoriously well known that compiling the configuration files for a firewall are used to performed the intended functionality, namely setting up a security policy that is to be enforced whereby the teachings of Grennan are relied upon for showing the use of a configuration file for a firewall since it is not explicitly disclosed by Reid et al.

The teachings of Reid et al are silent on the use of a memory for storing computer readable code and a processor coupled to memory that is configured to execute the computer readable code. The examiner hereby asserts that it would have been obvious that the teachings of

Reid et al comprise a memory for storing computer readable code and a processor coupled to memory that is configured to execute the computer readable code in order for the teachings to be performed as disclosed. The software program (computer readable code) and necessary hardware (processor and memory) to perform the necessary tasks are notoriously known to one of skill in the art as an essential part of computing. It is obvious that the teachings of Reid et al exist in the form of a software program (computer readable code) and are utilized by the hardware, namely stored in memory and a processor interprets, processes, and performs the task of providing policies for a plurality of regions to restrict communications to and from each of the regions as enforced by a firewall.

As per claim 30, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The teachings of Reid et al fail to disclose of translating of a configuration file for a firewall. It is disclosed by Grennan of setting up a configuration file for a firewall and compiling the kernel (section 4.2, 5.1). It is inherent that the configuration file would have been translated into a language that is used by the computer system since it is notoriously well known that different computing systems use different types of operating systems and there exists a need to convert a program into a language that is interpretable by a computing system using a different language from another. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a compiler.

for generating a configuration file for a firewall since it is known in the art that a configuration file for a firewall dictate the how the firewall functionality is to be performed. Although Reid et al is silent on the use of a compiler for generation (translating) of a configuration file, the teachings of Reid et al are suggestive of compiling wherein it is disclosed of ACLs (rules) used by the kernel for building, modifying, deleting, and querying the rules (col. 8, lines 20-23) which would need compiled. It is essential that a compiler for generating a configuration file in the format that is to be used by a system exists in the teachings since it is notoriously well known that compiling the configuration files for a firewall are used to performed the intended functionality, namely setting up a security policy that is to be enforced whereby the teachings of Grennan are relied upon for showing the use of a configuration file for a firewall since it is not explicitly disclosed by Reid et al.

As per claim 38, Reid et al discloses of communications (packets) to (send) and from (receive) each of the plurality of network interfaces (hosts) is restricted in accordance with a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface (host) is assigned. The firewall comprising a plurality of regions (assignment of roles) having policies (rules) is configured (generated) for each of the regions (assignment of roles)(col. 2, lines 8-17). Various commands (definitions) are shown by Reid et al for setting up access control rules that are applied to the regions (assignment of roles) in column 11, denoted in the upper part of the page. The teachings of Reid et al fail to disclose of generation of a configuration file for a firewall. It is disclosed by Grennan of setting up (generating) a

configuration file for a firewall (section 4.2). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a configuration file for a firewall since it is known in the art that a configuration file for a firewall dictate t*-3.he how the firewall functionality is to be performed. Although Reid et al is silent on the use of a configuration file, it is essential that a configuration file exists in the teachings since it is notoriously well known that configuration files for a firewall are used to performed the intended functionality, namely setting up a security policy that is to be enforced whereby the teachings of Grennan are relied upon for showing the use of a configuration file for a firewall since it is not explicitly disclosed by Reid et al.

The teachings of Reid et al are silent on the use of a memory for storing computer readable code and a processor coupled to memory that is configured to execute the computer readable code. The examiner hereby asserts that it would have been obvious that the teachings of Reid et al comprise a memory for storing computer readable code and a processor coupled to memory that is configured to execute the computer readable code in order for the teachings to be performed as disclosed. The software program (computer readable code) and necessary hardware (processor and memory) to perform the necessary tasks are notoriously known to one of skill in the art as an essential part of computing. It is obvious that the teachings of Reid et al exist in the form of a software program (computer readable code) and are utilized by the hardware, namely stored in memory and a processor interprets, processes, and performs the task of providing

policies for a plurality of regions to restrict communications to and from each of the regions as enforced by a firewall.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Green et al, U.S. Patent 6,332,195,

Ahlstrom et al, U.S. Patent 6,327,618,

Gooderum et al, U.S. Patent 6,219,707,

Antur et al, U.S. Patent 6,212,558,

Coss et al, U.S. Patent 6,154,775,

Nessett et al, U.S. Patent 5,968,176,

Green et al, U.S. Patent 5,913,024,

Gooderum et al, U.S. Patent 5,918,018,

Coley et al, U.S. Patent 5,826,014,

Shwed et al, U.S. Patent 5,835,726,

Wool et al, JP 02001237895A

Bartal et al, "Firmato: A Novel Firewall Management Toolkit"

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Revak whose telephone number is (703) 305-1843. The

examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703) 305-9711. The fax phone number for the organization where this application or proceeding is assigned as follows:

for After-Final Communications:	(703) 746-7238;
for Official Communications:	(703) 746-7239;
for Non-Official Communications:	(703) 746- 7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

NORMAN M. WRIGHT
PRIMARY EXAMINER
14 4213

CR

February 22, 2002